North Carolina State Government Statewide Initiatives and Strategies 2003-2005 Biennium

State CIO's Recommended Approach for Managing Information Technology for a Better North Carolina

December 19, 2002

North Carolina State Government
Statewide Initiatives and Strategies
2003-2005 Biennium

Table of Contents

A document containing supplemental materials relevant to this report is available from the IRM Division of ITS. Copies can be obtained by phone at 919-981-5510 or e-mail at irm@ncmail.net.

Acronyms:

CIO	Chief Information Officer
DR/BC	Disaster Recovery and Business Continuity
HIPAA	Health Insurance Portability and Accountability Act
IPPC	Information Protection and Privacy Committee of the IRMC
IRMC	Information Resource Management Commission
IT	Information Technology
ITS	Information Technology Services
LAN	Local Area Network
PC	Personal Computer
SIPS	State Information Processing Services
TAPCC	Technical Architecture and Project Certification Committee of the IRMC
TCO	Total Cost of Ownership
WAN	Wide Area Network

I. Executive Summary

North Carolina is at a crossroads for its management of information technology (IT) in state government. While several state agencies have received national recognition and awards for innovative services and applications, and where it once was aspiring to be one of the bellwether states for its farsighted implementation and use of IT for better government, North Carolina is now in a position of stagnation. The state has a choice: it can actively address pressing issues and challenges and provide positive and proactive leadership, or it can maintain the status quo of inefficient use of limited fiscal resources, excessive costs of IT operations, and lost opportunities to enable better government.

Budget crises; threats of terrorism; and citizen pressures for more responsive services, easier access to government, and greater stewardship for tax dollars are placing increasing demands for the cost-effective deployment and use of technology to serve the public better and save money. The state must build upon the successes of past agency endeavors, statewide consolidations, and leadership provided by the executive and legislative branches and the Information Resource Management Commission (IRMC) to address the present challenges and opportunities for improvement. It must adopt bold and results-driven statewide initiatives and execute achievable and targeted strategies that maximize the benefits from limited fiscal, personnel, and hardware/software resources by achieving more value from fewer dollars.

In summary, the state must change its approach for the management of IT in state government. Now is the time to implement a new statewide IT management model that will respond proactively to the present realities, as well as establish a long-term framework for integrating technology into the ways the state conducts business to enable a more efficient and citizen-oriented government.

Relevant facts

The following facts reflect the technical, business, governmental, and economic realities facing the state.

1. Technology is essential for the successful performance of the state's business processes and program operations.

2. Over the past decade, technology has evolved from a mainframe-centric structure to a networked computing environment of more distributed IT assets.

3. The real and increasing threat of malicious and damaging attacks has heightened the need for the protection of the state's valuable IT assets through cost-justified security measures.

4. Disasters (from either human-originated or natural causes) can have adverse consequences for the conduct of business processes and program operations; therefore, the state must have the ability to quickly recover data and other mission-critical IT assets and to continue business until the situation can be restored to normalcy.

5. Nationally, the states are facing the direst fiscal crisis in nearly half a century. North Carolina has been particularly hard hit due to its unique set of unfortunate circumstances.

6. Budget shortfalls are beginning to cause adverse repercussions on the state's IT infrastructure and mission-critical applications.

7. Compared to other states similar in population, budget, and IT funding (ranking eleventh in each of these categories), North Carolina has not received the maximum value from the state's investments in IT resources.

8. While funding for IT is important, the management of IT is critical, especially under conditions of constrained budgets.

Mandate – The state must change its approach for the management of IT in state government.

The new management approach is necessary to:

- Acknowledge and reflect economic realities.

- Achieve maximum utilization of scarce fiscal, personnel, and hardware/software resources.

- Realize economies of scale in optimizing common services and shared infrastructure and leveraging purchasing power.

- Provide for efficient business processes and the best possible program outcomes.

- Satisfy new and increasing requirements for reliable operations, security of assets, confidentiality of data, and disaster recovery and business continuity for essential infrastructure and mission-critical systems.

Approach – Manage IT as a statewide utility

Citizens are continuing to ask for new and expanded services, and they are demanding greater productivity of personnel and more accountability for expenditures and program results. Technology can enable the state to meet these requirements, but only if it is deployed and used effectively. This is a difficult task, as IT is not self-managed, inexpensive, or easy to control. Rather, it is complex and expensive. It demands constant attention and requires difficult decision-making.

Agencies have the program knowledge and client perspective to satisfy their individual business needs and program objectives. The knowledge, skills, and expertise of their personnel are concentrated in the areas of governmental imperatives, business rules, and program performance factors.

In the mainframe era, the state recognized that computers and telecommunications were utility functions that could be best provided from a common organization. ITS (formally called SIPS) was formed in the early 1980s to effect the consolidation of agency mainframes and networks. As a result, the sharing of the technical expertise of a single pool of personnel and the use of common facilities offered cost savings through the more efficient use of staff resources and economies of scale, while allowing modern technology to be available to all agencies.

The utility model for managing statewide IT resources was not extended to the networked computing environment featuring distributed assets (such as LANs, servers, PCs, etc.). Agencies purchased, implemented, and operated local computing hardware/software resources and telecommunications equipment, and they connected these devices and systems to the state's common wide area network (WAN) to communicate electronically among the devices and systems.

Like many public and private entities, the state has attempted to cope with the evolving heterogeneous technical environment of geographically dispersed IT assets by developing policies and setting standards for coordinating efforts, providing quality control, and making agency systems and statewide infrastructures work together. This approach has not worked as desired. The state is experiencing duplications of investments, increased

operating costs, less reliability of processing, higher hardware/software purchase prices, excessive system implementation costs, and increased security exposures.

North Carolina must extend the utility approach to the statewide management of the new technical environment of distributed IT assets, which are now under agency direction. This new approach for the statewide management of IT is in line with lessons learned and recent actions taken by leading companies in the private sector, the federal government, and other states.

Action Plan – Establish initiatives and strategies for implementing the utility approach for the statewide management of IT in state government.

To move to the statewide utility model for managing IT in North Carolina state government, the Governor and the IRMC must accomplish the initiatives and strategies highlighted below. The initiatives and strategies form the outline of a more detailed plan that must be developed for implementing them. The plan must be action-oriented, task-specific, responsibility-driven, and timetable-delineated. Each initiative is essential; therefore, the numerical order is not significant from either priority or sequencing viewpoints.

First Initiative – Manage all of the state's IT hardware/software assets from more of a statewide perspective.

> **Strategy 1** – Implement a statewide asset repository for collecting and maintaining a complete, accurate, and up-to-date inventory of the state's hardware/software and telecommunications equipment assets, including the designated mission-critical applications and assets supporting them.
>
> **Strategy 2** – Adopt statewide configuration standards for commonly used assets (such as servers, PCs, and LANs); adopt best practices, standards, and tools for managing them; and develop purchasing policies to maximize volume and service discounts and warranties.
>
> **Strategy 3** – Consolidate the management of the state's multiple server-based data centers, beginning with the development of a work plan and timetable that must be submitted for approval by the State CIO. Employ best practices, standards, and performance reporting.

Strategy 4 – Develop a statewide portfolio management approach for identifying, evaluating, and selecting IT investments. The intent is to eliminate duplication; realize synergies from multiple funding sources and projects; leverage past and future investments in common shared infrastructure; and invest in projects that provide the least risks, best value, and most benefits to the state.

Second Initiative – Manage more closely the state's implementation of IT projects.

Strategy 1 – Develop processes and procedures for the State CIO to verify that agencies have the necessary staffing resources, processes, and tools to successfully perform IT projects (especially for the management of outside contractors) before the projects can be certified by the IRMC. Before projects can begin, the State CIO must approve the management plan and technical approach, including personnel assignments (with responsibilities/accountabilities), management process, development life cycle, work plan, risk analysis, quality assurance, budget analysis, and technical architecture.

Strategy 2 – Restructure the IRMC's project certification, reporting, and quality assurance policies and procedures to incorporate more intensive and timelier reviews by the State CIO, as the projects move through their life cycles. The State CIO must develop practices and contribute staffing resources for assisting agencies to perform high-risk projects successfully.

Third Initiative – Develop a comprehensive statewide outsourcing strategy by expanding lessons learned from past successful efforts.

Strategy 1 – The State CIO must develop a comprehensive framework for analyzing potential outsourcing alternatives.

Strategy 2 – As appropriate, the state must consider outsourcing opportunities where viable and cost-effective.

Fourth Initiative – Provide the most cost-justified protection against unwanted events from human and natural sources, and make available capabilities for disaster recovery and business continuity should the need occur.

Strategy 1 – The State CIO must make available cost effective statewide security management services for the agencies, including research and assessment, consulting assistance, secure networked

computing facilities, intrusion detection and response, and other services desired for ensuring the integrity of data and strategic IT assets.

Strategy 2 – The state must develop adequate disaster recovery and business continuity provisions for its computing and telecommunications assets and its mission-critical systems, with current and tested policies, procedures, and off-site backup facilities. Applications using distributed (non-mainframe) computing hardware/software and locally based telecommunications equipment must receive particular attention, as they are not adequately covered under current practices and capabilities.

Fifth Initiative – Find adequate, consistent, and reliable funding sources for IT investments and operations and the management of these.

Strategy 1 – Develop provisions for enterprise infrastructure funding that provides common technical services and shared technical infrastructure including security services and disaster recovery/business continuity for all agencies and all programs.

Strategy 2 – Develop provisions for ongoing funding for operating and maintaining (or replacing/updating) mission-critical systems and applications, especially those at risk due to obsolescence or lack of technical support.

Strategy 3 – Develop procedures (including the involvement of the State CIO, State Budget Officer, and State Controller) for reviewing funding requests (regardless of source) and examining ongoing funding certifications and expenses from the statewide perspective to eliminate duplication of investments, minimize statewide IT operating expenses, and ensure adequate infrastructure is available for and used by all agencies.

Sixth Initiative – Recruit and retain a proficient and appropriately staffed IT workforce.

Strategy 1 – Research, develop, and fund programs for attracting and retaining qualified IT professionals, including competitive payment for required skills and abilities.

Strategy 2 – Ensure that agency technical staff and support personnel receive sufficient training to maintain agency IT assets and applications and acquire the knowledge and interpersonal skills

necessary to adapt quickly to new technologies and the changing workplace environment.

Conclusion

State technology leaders must manage IT as a statewide utility in order for state agencies to: cut costs and achieve on-going savings, deliver more value to the taxpayers from IT investments and do so in shorter time periods, strengthen security infrastructures and expand disaster recovery and business continuity capabilities, become more citizen-focused in decision-making, and produce better results from program operations.

II. Purpose, Background, New Management Approach, and Goals and Objectives

Purpose and Background

The primary purpose of this Initiatives and Strategies document is to present the outline of a North Carolina's strategic technology plan in the form of key initiatives and the associated strategies to achieve them. This document provides the foundation for the development by the State CIO of a more detailed implementation plan that must be action-oriented, task-specific, responsibility-driven, and timetable-delineated.

Today, the state is in a position of having to take one of two clear choices regarding its statewide management of IT in state government:

1. Take strong and proactive leadership to face the daunting challenges presented by a severe and chronic budget crisis, ever-changing technology innovations, and continually rising citizen expectations for more responsive (yet less costly) programs and services, or

2. Continue with the status quo to let events and circumstances overtake management actions and dictate the impact of the economic, business and technical environments on the health and welfare of IT in state government.

In developing the statewide initiatives and related strategies for the management of technology, the following facts must be considered. They reflect the technical, business, governmental, and economic realities facing the state.

Fact 1 – Technology is essential for the successful performance of the state's business processes and program operations.

Information technology is an inextricable and essential part of the workings of state government. Properly funded and appropriately used, it can offer the following advantages to the public:

- Facilitate easier access to and more responsive interaction with state agencies.

- Increase productivity of program operations and improve efficiencies of business processes.

- Improve the value of and benefits from state programs.

- Contribute to educational opportunities, public safety and welfare, and economic development and quality of life.

Fact 2 – Over the past decade, technology has evolved from a mainframe-centric structure to a networked computing environment of more distributed IT assets.

The mainframe era featured a few high-powered and centrally located and managed computing and data storage facilities, with dedicated connections to rigid access devices. Today's networked computing environment consists of many geographically dispersed and locally managed computing and data storage devices interconnected with local and wide area networks and offering ubiquitous access from a multitude of computing and telecommunications devices. The new technology environment offers great benefits, however; it creates many additional management challenges.

Fact 3 – The real and increasing threat of malicious and damaging attacks has heightened the need for the protection of the state's valuable IT assets through cost-justified security measures.

Protecting the state's computer and telecommunications infrastructure and its mission-critical applications has never been more important because of concerns about attacks from individuals and groups with malicious intent, including terrorism. These concerns are well founded for a number of reasons, and they can originate from a variety of sources, including cyber-terrorism accomplished through readily available hacking tools and more sophisticated attack technology. In addition, security precautions are necessary to prevent data tampering, fraud, and inappropriate disclosure of sensitive information.

Fact 4 – Disasters (from either human-originated or natural causes) can have adverse consequences for the conduct of business processes and program operations; therefore, the state must have the ability to quickly recover data and other mission-critical IT assets and to continue business until the situation can be restored to normalcy.

As with other large governmental and private organizations, state agencies rely extensively on computerized systems, interconnected networks, and

electronic data to support their missions, deliver vital services and perform necessary functions. Accordingly, appropriate provisions must be made for disaster recovery and business continuity, especially for common shared IT infrastructure and mission-critical applications.

Fact 5 – Nationally, the states are facing the direst fiscal crisis in nearly half a century. North Carolina has been particularly hard hit due to its unique set of unfortunate circumstances.

Even after using its rainy day funds and undergoing extensive budget cuts, the state may need to solve an approximately $2 billion projected budget deficit for the coming 2003-2004 fiscal year. Only four states cut their fiscal year 2002 - 2003 budgets more than North Carolina. (Source: NGA Report The Fiscal Survey of States, November 2002) Moreover, the state budget situation is likely to remain bleak for at least two more years, if not longer.

Fact 6 – Budget shortfalls are beginning to cause adverse repercussions on the states IT infrastructure and mission-critical applications.

IT has experienced deep and continuing budget shortfalls. This has presented problems because of the insufficiency and aging of technical infrastructure (creating at-risk systems), the growth in the backlog of applications to improve services to citizens (especially self-service using the Internet), and the decreased reliability and dependability of operations (creating more down-time for public services). The increasing rate of retirements and the lack of adequate funding to fill vacancies are exacerbating at-risk situations.

Fact 7 – Compared to other states similar in population, budget, and IT funding (ranking eleventh in each of these categories), North Carolina has not received the maximum value from the state's investments in IT resources.

North Carolina's IT budget is comparable percentage wise and in absolute amounts to other states of similar size. The problem is that North Carolina has not compared favorably to other states in the results obtained from the state's investments in IT. For example, through the Digital States Survey, the Center for Digital Government and the Progress and Freedom Foundation have ranked the states by progress in bringing digital technology into the business of government. In the past three reports, North Carolina was not in the top 25 states in 1998 and 2000, and it was 25th in the just released 2001 rankings.

Fact 8 – While funding for IT is important, the management of IT is critical, especially under conditions of constrained budgets.

While the state may not have invested enough in IT over the years, the economic realities are that a sufficient amount of additional funding will not be available in the foreseeable future. In addition, North Carolina has not maximized the value of the state's IT expenditures. It is not necessarily how much an organization spends on IT that determines the benefits received – it is how the organization deploys and uses IT and how it manages IT that counts.

New Management Approach

The core competencies of agencies are to accomplish their missions and implement their strategies while performing successfully business processes and program operations. The knowledge, skills, and expertise of their personnel are concentrated in the areas of governmental imperatives, business rules, and program performance factors.

In the mainframe era, the state (like many public and private entities) recognized that computers and telecommunications were utility functions that could be best provided from a common organization. ITS (formally called SIPS) was formed in the early 1980s to effect the consolidation of agency mainframes and networks. As a result, the sharing of the technical expertise of a single pool of personnel and the use of common facilities offered cost savings through the more efficient use of staff resources and economies of scale, while allowing modern technology to be available to all agencies.

The utility model for managing statewide IT resources was not extended to the networked computing environment featuring distributed assets (such as LANs, servers, PCs, etc.). Agencies purchased, implemented, and operated local computing hardware/software resources and telecommunications equipment, and they connected these devices and systems to the state's common wide area network (WAN) to communicate electronically among the devices and systems. This approach led to a proliferation of hardware and software choices with resultant support cost increases and new problems with interoperability.

From a statewide perspective, the management of this heterogeneous environment of geographically distributed IT assets has been pursued through enterprise policies and standards. While effective to some extent, the demand to become more efficient in response to the severe budget crisis; increasingly compelling needs for security, disaster recovery, and business

continuity; and troubles experienced by the agencies in implementing and operating the new technologies have exposed serious and chronic problems with this management approach.

The state must extend its utility model for the statewide management approach for IT to incorporate distributed IT assets. That is, the state must radically change its approach to the statewide management of its networked computing technical environment from treating it as an agency-by-agency resource to a perspective of a statewide utility that serves a useful purpose in:

- Enabling agencies to achieve state strategies, governmental mandates, and program goals and objectives.
- Providing common services and shared infrastructure to all agencies, featuring lowest cost, proven security, and better reliability.
- Offering high-levels of customer service to the agencies.

The new utility-focused management approach is necessary to:

- Recognize and reflect economic realities.
- Achieve maximum utilization of scarce fiscal, personnel, and hardware/software resources.
- Realize economies of scale in optimizing common services and shared infrastructure and leveraging purchasing power.
- Provide for efficient business processes and the best possible program outcomes.
- Satisfy in the most cost-effective manner new and increasing requirements for reliable operations, security of assets, confidentiality of data, sensitivity of information, and disaster recovery and business continuity for essential infrastructure and mission-critical systems.

Goals for Managing IT as a Statewide Utility

Citizens expect that the state will cost-effectively deploy and use technology to meet the expanding needs of the emerging digital environments, including schools, workplaces, health centers and homes. Today, citizens are not just customers of government services, but shareholders of government. They expect a government that is citizen-centric, cost-conscious, service-based, responsiveness-driven, and change-oriented. The goals for managing IT as a statewide utility listed below are responsive to the needs and expectations of the public served by the state.

The primary goals for managing IT as a statewide utility are:

Goal 1 – Leverage IT as a strategic asset for simplifying public access to and interaction with the government and for enabling better government that is more productive, less costly, and closer aligned with the hopes, desires, and aspirations of its citizens.

Goal 2 – Promote the availability of and build upon the foundation of common technology services and shared technology infrastructure to employ economies of scale for maximizing reliability, performance, security, and disaster recovery and business continuity, while minimizing implementation and operating costs.

Goal 3 – Provide for the cost-justified security of IT assets and the recoverability of common, shared infrastructure and mission-critical systems and applications.

Goal 4 – Provide for a proficient state government IT workforce through innovative and appropriate recruitment, retention, and training efforts.

Goal 5 – Identify and remedy infrastructure components and applications that are mission-critical and at-risk to preserve the integrity of the state's business processes and the credibility and trust of the public for program operations.

Goal 6 – Take advantage of all viable outsourcing options for providing and delivering IT services to address business problems and program challenges.

Introduction to Initiatives and Strategies

Six initiatives and their associated strategies have been identified for establishing the groundwork for the first path of action (strong and proactive leadership) and accomplishing the goals described above. These initiatives and strategies are described in detail in the following chapter of this document. They will lead the state to the management of IT as a statewide utility. This will enable the achievement of state strategies, governmental mandates, and program goals and objectives, and provide common services to all users. In this manner, the state will be able to achieve maximum benefit at least costs from its fiscal, personnel, and strategic IT asset resources and mission-critical systems and applications.

The six initiatives originated primarily from work with the agencies, including the review of agency expansion budget requests and the examination of agency IT plans. Additional insight resulted from research of materials from leading IT advisory service organizations and current literature, and direct discussions with and input from the ITS management team. These initiatives and strategies are in concert with the challenges of The Agency Technology Plan for ITS, which is included in this document as an appendix.

III. Major Initiatives and Associated Strategies

To move to the statewide utility model for managing IT in North Carolina state government, the Governor and the IRMC must accomplish the initiatives and strategies highlighted below. While many of these initiatives are a continuation of past efforts, several are new or emerging issues that must be addressed in a thorough and expeditious manner.

The initiatives and strategies form the outline of a more detailed plan that must be developed for implementing them. The plan must be action-oriented, task-specific, responsibility-driven, and timetable-delineated. The initiatives are all essential (individually and collectively); therefore, the numerical order is for organization only – it does not indicate rank, priority or sequence.

First Initiative – Manage all of the state's IT hardware/software assets from more of a statewide perspective.

Description

The foremost objective of the management of IT is to select, implement and operate IT investments that best meet state governmental initiatives, agency missions, and program goals in the most cost-effective manner. Two fundamental concepts are central to satisfying this imperative.

- Statewide approach – IT investments must be planned, implemented and managed from a broad-based statewide perspective rather than a more narrowly focused agency, program or application view. The primary intent is to maximize the use of common technical services and shared technical infrastructure to realize cost savings; facilitate the sharing of information; and achieve higher levels of integrity of data, reliability of operations, security of assets, and disaster recovery and business continuity through:

    - Synergy – combining fiscal, personnel and hardware/software resources to obtain collectively capabilities that could not be afforded or accomplished individually.

- ♦ Leverage existing infrastructures, knowledge, experiences, and processes to develop new capabilities faster and more economically and eliminate costs of unnecessary duplication.

- ♦ Economies of scale – reducing unit (transaction) costs by sharing the same commonly used technical services and infrastructure (i.e., spread fixed costs over aggregated transactions from multiple sources and applications).

- ♦ Critical mass – building a sufficiently robust infrastructure to handle scale (new users), flexibility (changes in requirements), and extensibility (new technologies) in a timely and economical manner.

- Total cost of ownership (TCO) – This is the total life cycle (lifetime) cost of an asset from its purchase through implementation, operation, and retirement/disposal. For IT assets, TCO costs typically include (a) capital (e.g., purchase price); (b) implementation/installation, (c) maintenance and technical support, such as, monitor, fix, update, maintain, etc.; (d) administrative (e.g., purchasing, contracting, etc.); and (e) end-user support, such as training, service center (help desk), and other user assistance.

A major area of concern is the state's vast multi-million dollar investment in common shared infrastructure, mission-critical applications, and distributed IT assets (such as PCs, LANs, servers, and printers). The following problems illustrate the risks being experienced and opportunities for potential dollar savings being foregone through the state's present practices for managing its strategic hardware/software and telecommunications assets.

- The state is spending too much money supporting its distributed IT assets by not using a statewide approach for managing them:

  - ♦ Little or no statewide coordinated management and no cost/performance awareness at the statewide level or at the agency level (i.e., no identified responsibility or accountability for costs or performance/results of these investments at statewide or agency levels).

  - ♦ Little or no sharing of common assets or management tools, resulting in the duplication of infrastructure assets and personnel to manage them.

- Difficulty in and excessive expenses associated with performing large-scale projects involving statewide rollouts of hardware/software in environments presenting diverse and disparate technical infrastructures due to lack of knowledge of present equipment and personnel capabilities.

- There is no statewide inventory (and very few agency inventories) of computing hardware, communications equipment, or software assets. Such an inventory could contain the following information about these assets.

    - What it is.

    - Where it is located.

    - What it cost.

    - What it is used for; number of users; and degree of criticality for accomplishing governmental initiatives, agency missions, and program goals.

    - Warranties, maintenance terms and conditions, software licenses, maintenance contracts and fees, etc.

    - Detailed technical characteristics.

    - Benefits received and performance to date of assets.

    - Number and types of interfaces with other applications and data exchanged.

    - Number of personnel and types of personnel skills required to support.

- The state has little or no knowledge of expenditures (TCO) for IT assets. Ongoing support costs generally exceed capital outlays for distributed IT assets.

    - Capital outlay is typically around 40% of TCO.

    - Operating, support and maintenance is typically around 60% of TCO.

- The state is potentially exposed to unacceptable risks in the following areas.

    - Security of assets, confidentiality of data and privacy of individuals.

    - Disaster recovery and business continuity.

    - Operational reliability, applications availability, and ability to respond to change quickly and economically.

    - Accountability for investments (costs and benefits).

    - Large-scale application development projects, especially those involving statewide rollouts.

- The state does not have a formal process for consolidating funds from various sources and combining investments from multiple agencies or programs from a statewide perspective to gain the greatest benefits for all. As a result, IT investments are not made in a synergistic manner among agencies and programs leading to excessive costs. For example, much hardware and software is purchased on an individual basis, which minimizes potential volume discounts from the standardization of assets and the aggregation of demand. Also, tools and staff are unnecessarily duplicated among agencies. Due to wasting money by not employing the statewide utility approach for managing IT, we do not have the funds to accomplish projects or conduct operations correctly, leading to increased risks and the potential for more failures. This is a structural problem – not a nefarious people issue.

  Potential IT investments must be identified, evaluated, and selected based on a variety of criteria, including accomplishing legal mandates and governmental initiatives, fulfilling agency strategies and program goals and objectives, and delivering the most useful purposes or best values considering costs, risks, and benefits. A formal statewide view of potential IT investments must be conducted to weed out duplication, identify potential opportunities for building or using common shared infrastructure, and finding ways to combine funds for best meeting multiple business or program needs. Although it is not the role of technologists to judge the merits of IT investments among individual agencies or programs, the opportunity for meeting statewide needs may

influence priority-sequencing decisions. Therefore, a statewide view, using portfolio management techniques, should be used to rank potential IT investments.

A business case analysis should be performed for major potential IT investments. At least four key areas should be examined:

- Total cost of ownership over the asset's lifetime or a reasonable period (such as five years).
- Expected benefits or value, which may include monetary aspects, such as cash flow calculations (return on investment, payback period, internal rate of return, etc.) and non-monetary aspects, such as legal mandate, public good will, prerequisite for a succeeding high-value investment, etc.
- Technical feasibility, such as agreement with the statewide technical architecture, agency technical architecture, etc.
- Risks, including implementation, governmental, economic, etc., as well as the foregone opportunities of not making the investment.

Implementation Strategies

The following implementation strategies follow the recognized best practices in both governmental and private sectors for the strategic management of IT assets.

Strategy 1 – Implement a statewide asset repository for collecting and maintaining a complete, accurate, and up-to-date inventory of the state's hardware/software and telecommunications equipment assets, including the designated mission-critical applications and assets supporting them.

Strategy 2 – Adopt statewide configuration standards for commonly used assets (such as servers, PCs, and LANs); adopt best practices, standards, and tools for managing them; and develop purchasing policies to maximize volume and service discounts and warranties.

Strategy 3 – Consolidate the management of the state's multiple server-based data centers, beginning with the development of a work

plan and timetable that must be submitted for approval by the State CIO. Employ best practices, standards, and performance reporting.

Strategy 4 – Develop a statewide portfolio management approach for identifying, evaluating, and selecting IT investments. The intent is to eliminate duplication; realize synergies from multiple funding sources and projects; leverage past and future investments in common shared infrastructure; and invest in projects that provide the least risks, best value, and most benefits to the state.

Second Initiative – Manage more closely the state's implementation of IT projects.

Description

Successful project management should deliver projects on time, within budget, aligned with business goals and program objectives, and provide the economic benefits and governmental values expected. Unfortunately, many IT projects fail to meet performance expectations because of a wide variety of factors, including high risks, excessive project size, faulty planning, inaccurate estimating, incomplete requirements, and inadequately defined project scope. Other factors contributing to failed projects include deficient or inexperienced project management, poorly written contracts and failure to manage contractors properly, undefined executive sponsorship, unclear responsibility and accountability assignments, incomplete change management procedures, and scope creep.

The state has had a long and distinguished history of monitoring, accounting for, and reporting major information technology projects. However, recent problems with large-scale statewide rollout projects have revealed critical weaknesses in the ability of agencies to manage complex IT investments appropriately. All technology projects have inherent problems; however, the nature of statewide multi-jurisdictional projects amplifies the risks.

Past project certification, review, and oversight efforts have been accomplished under the auspices of the IRMC, especially its Technical Architecture and Project Certification Committee (TAPCC). The policies and procedures of the IRMC's Project Certification, Progress Reporting and Quality Assurance process govern the project approval and monitoring activities.

Improvement efforts for statewide project management must address the following objectives:

- Intensify the focus on areas of higher risk to identify sooner critical problems or troubled projects.

- Assign the responsibilities and accountabilities for project performance more precisely to encourage the early resolution of key issues or problems.

- Make the project reporting and quality assurance process more cost-effective by substituting the verification and validation of project status through the use of ITS staff in situations where outside, independent quality assurance reviews are not warranted.

- Obtain a better understanding of the projects, including critical success factors and dominant organizational, business, and technical issues through comprehensive visibility/risk profiles.

- Obtain a more comprehensive portfolio of state IT projects, leading to more complete knowledge, understanding, and reporting of these efforts.

- Examine the business case or justification for each project periodically as it is being implemented to confirm the expected costs, timetables, values, and benefits are still valid and whether it should be continued and finished.

Offer more assistance to the agencies for project management and for developing staff and for selecting and implementing tools to achieve greater proficiency in project planning and management. Where appropriate, consider sharing common tools, methodologies, and processes to obtain economies of scale, reduce duplication, and leverage scarce and expensive personnel and fiscal resources.

Implementation Strategies

The state must build upon its extensive history of lessons learned to develop a new statewide model for project management. This model is required for consistent and predictable success in implementing IT projects, and it must address the areas of governance, policies and standards; measurements; methodologies; approval, reporting, and evaluation processes; and fiscal, personnel, and technical resources. The following two strategies will form key components of the statewide project management model.

Strategy 1 – Develop processes and procedures for the State CIO to verify that agencies have the necessary staffing resources, processes, and tools to successfully perform IT projects (especially for the management of outside contractors) before the projects can be certified by the IRMC. Before projects can begin, the State CIO must approve the management plan and technical approach, including personnel assignments (with responsibilities/accountabilities), management process, development life cycle, work plan, risk analysis, quality assurance, budget analysis, and technical architecture.

Strategy 2 – Restructure the IRMC's project certification, reporting, and quality assurance policies and procedures to incorporate more intensive and timelier reviews by the State CIO, as the projects move through their life cycles. The State CIO must develop practices and contribute staffing resources for assisting agencies to perform high-risk projects successfully.

Third Initiative– Develop a comprehensive statewide outsourcing strategy by expanding lessons learned from past successful efforts.

Description

IT outsourcing can be described as the activities associated with acquiring IT services from one or more external providers. During outsourcing, a client organization transfers responsibility for executing one or more IT services to one or more external providers. This responsibility is executed through control and management of the processes, people, and technology associated with these services.

While IT outsourcing (either the entire IT function or selected services) has been a popular practice in the private sector for the past 10 years, it has just recently become a more common event in the public arena. The federal government has led the effort for some time with several large-scale contracts, and recently the rate and depth of outsourcing relationships by federal agencies have expanded significantly.

State and local governments have been much slower to adopt IT outsourcing; however, Pennsylvania (data centers), California (network/telecommunications), Virginia (seat management), and Florida (human resources) have all elected to outsource a portion of their technology infrastructure to an external provider of services. North Carolina has been an early leader in the outsourcing of its voice, data, and video

telecommunications. Few state and local government organizations have elected to outsource their entire technology infrastructure to a single vendor.

In light of the risks involved, many companies and state and local governments are deciding to keep their main IT capabilities in-house, but considering or engaging in selective outsourcing. Good candidates for this are commodity services, such as telecommunications and seat management, which exhibit the characteristics listed below.

Characteristic	Benefit
Outsourcing availability from several competing suppliers.	Provide price competition.
Specifications easy to determine.	Enable contract performance or service level expectations that are easier to draft; better understood by all participants; and simpler to measure, report, and monitor.
Services involve technologies or processes with which the organizations lack expertise or funding to implement the required technology infrastructure or do well with present staff.	Offer the potential for obtaining the services at less cost and/or higher quality than available in-house.

The sourcing framework may consist of several phases. These include defining the sourcing strategy; clarifying the operational model and developing the contractual provisions; evaluating bids, selecting the provider, and completing the contract; transitioning to the provider; and managing the vendor and ensuring services are provided. Key prerequisites for any sourcing arrangement are:

- Develop strategic objectives - The capabilities and costs of in-house supported operations must be known, and the business reasons (goals and objectives) for outsourcing must be understood and agreed upon. Moreover, the desired degree of control over IT operations supporting business processes and program operations must be determined.

- Determine cost implications – An in-house supplier must only break-even, an outsource provider must make a profit. Therefore, in the long run, the outside provider should be more expensive. However, due to budget constraints, investment capital may not be

available and/or operating funds may not be sufficient to support quality in-house services, so that outsourcing may be the only viable economic alternative.

- Evaluate quality expectations – Service level expectations (the extent of the need for stable, reliable and flexible operations) must be determined. Alignment between IT operations and business needs and program requirements must be understood. Outsourcing will not solve wide variations between types and quality of services delivered by the in-house IT organization and the desires of the business areas or program groups.

In summary, before outsourcing alternatives can be contemplated, present IT operations costs must be known, IT processes must be documented, business and IT problems and challenges must be recognized, and risks for both internal and outsourced approaches must be identified and evaluated. In addition, competitive offerings must be researched, and cost-benefit analyses performed for in-house and outsourced alternatives.

Implementation Strategies

The state has outsourced its telecommunications services for many years. These contracts have provided the high quality services at the most competitive prices. This year, ITS negotiated a seat-management contract with several vendors; offering this service as an agency and local government option. Internal studies have been conducted in other areas offering potential for outsourcing to assist in developing strategies, evaluating options, and determining future steps. The strategies below build upon the experiences gained from past and current outsourcing experiences.

Strategy 1 – The State CIO must develop a comprehensive framework for analyzing potential outsourcing alternatives.

Strategy 2 – As appropriate, the state must consider outsourcing opportunities where viable and cost-effective.

Fourth Initiative – Provide the most cost-justified protection against unwanted events from human and natural sources, and make available capabilities for disaster recovery and business continuity should the need occur.

Description

Security

While the security of assets, value and confidentiality of data, and sensitivity of information have been imperatives for plans and operations of the state for years, the terrorist events of September 11, 2001 and the increasing number and sophistication of cyber attacks in the ensuing months have elevated security to the highest level of interest for state government and ITS. The foundation for the state's technology security plan is contained in G.S. 147-33.82, adopted in late 2001. Security related statutes prescribe responsibilities for the State CIO to set security standards and review agency compliance with them, while the State Auditor is responsible for conducting vulnerability assessments.

The state has adopted a results-oriented management framework to guide security efforts and a risk-management approach to identify specific security requirements. Risk management is accomplished by assessing threats and vulnerabilities (weaknesses) to the state's IT assets and evaluating and priority sequencing the IT infrastructure and applications to determine relative importance for protection from undetected exploits or obvious attacks. Results-based plans measure the effectiveness or performance of security related efforts.

Typically, the determination of required degrees of security involve trade-offs. Increasing security often necessitates higher costs and less convenience to citizens and employees for accessing information. Greater security also offers better privacy, more assurance of the integrity and confidentiality of data, and increased reliability of computing and telecommunications. Less security may allow fewer dollar investments in protective infrastructure, with increased availability of information. A reduction in security also increases risks of data compromise and decreases the reliability of processing.

The state has progressed steadily and produced many good and significant accomplishments in security awareness, policies, standards, and common services in the past year, especially through the ITS Security Office and the IRMC's Information Protection and Privacy Committee (IPPC). However, security is an ongoing effort, with the program involving a compilation of past work and new activities. Although perfection will never be reached, the state must fortify its resolve and intensify its efforts to obtain an acceptable balance between the level of security desired by its citizens and affordability to its taxpayers. Future plans must focus on conveying the urgency of implementing an adequate and appropriate security program. They must incorporate a shift in emphasis from a reactive and defensive position (threat determination) to a more proactive and offensive approach (vulnerability assessment). In this regard, state leaders must be made aware of the need

for more personnel and fiscal resources to obtain sufficient security for IT assets.

Key aspects for future security related efforts must include:

- Move faster - Threats are increasing dramatically and vulnerabilities are changing rapidly. It is time to transition from planning to implementation. In particular, assessments must be expedited and audits completed. Following findings and recommendations, the state must move quickly to remediation.

- Continue to move with expediency to protect against known potential vulnerabilities – Homeland Security, the Federal Bureau of Investigation (FBI), and other reputable organizations have identified the highest priority security vulnerabilities that should be addressed. While many vulnerabilities can be mitigated, complete removal of all of them is impossible. Any entity connected to the Internet is vulnerable to cyber attack.

- Intensify education and awareness efforts – Government leaders and key agency management personnel must understand and appreciate the risk management approach, urgency of actions and funding requirements of a successful security program. Agency personnel must be trained concerning information security standards.

- Assist agencies in implementing the risk-based security zone approach – This is an essential follow-up activity to the assessments and audits. The security zone concept allows agencies to apply the appropriate level of security, based on a balance of costs and risks (i.e., threats, vulnerabilities, and importance of assets to agency missions, including the need for confidentiality of data, privacy of individuals, and ease of access to information).

- Employ the enterprise approach for securing the state's IT infrastructure – Develop or obtain services needed by the agencies and provide them in a cost-effective manner, leveraging the security zone approach. Services include more secure computing and networking, intrusion detection, firewalls, virus prevention, forensics, encryption, etc.

- Search for and obtain outside fiscal resources – The state's budget crisis is limiting the availability of appropriated funds; therefore,

financing must also be obtained from federal grants and other sources.

Disaster Recovery and Business Continuity

With a history of ice storms, tornadoes, hurricanes, and floods, North Carolina's susceptibility to widespread disasters is well recognized. The threat and the potential for other equally serious devastating events increase with the advent of cyber, nuclear, chemical, biological and physical terrorism. The problem is compounded for IT in that local and isolated events (such as electrical outages, fires, plumbing failures, malicious acts, and human error) may cause severe disruptions to statewide business processes and program operations for extended periods of time.

While other IT investments and initiatives are desirable and have broad-based support (especially in times of budget shortfalls), effective disaster recovery and business continuity (DR/BC) strategies and plans are important, from both IT-centric and program-focused perspectives. For state government, extended outages of business operations caused by unwanted events may create a loss of revenue collections, an inability to carry out social programs, the obstruction to public safety, an impediment to business and democratic processes, and the diminishing of trust and confidence of the public. Moreover, new government regulations and initiatives, such as the Health Insurance Portability and Accountability Act (HIPAA) and Homeland Security, are imposing requirements for DR/BC.

Circumstances necessitate that state government entities have DR/BC plans that are adequate in scope of coverage; reflect appropriate threat assessments and vulnerability studies; and address personnel, procedural, and technological issues. Also, plans must be realistic and achievable, supported from top-to-bottom of the state governance and agency organizational structure, updated as conditions change, and tested periodically and when modified. Even minute changes to IT asset configurations, processes or procedures must be incorporated in DR/BC plans and tested.

ITS has done a good job with the recovery of mainframe applications, using the utility approach of sharing common facilities and procedures among multiple agencies and systems. For the mainframe-based systems, records and data are copied and stored at an off-site facility, and an alternate computing facility ("hot site") is available for processing if required. Drills are conducted regularly to ensure mission-critical applications can be bought on line within 24 hours. The DR/BC model for the mainframe needs to be

followed for the state's geographically dispersed distributed hardware/software assets.

Implementation Strategies

Implementation strategies for security and DR/BC must build upon current efforts, and they must take into account the considerations and requirements described above.

> **Strategy 1** – The State CIO must make available cost effective statewide security management services for the agencies, including research and assessment, consulting assistance, secure networked computing facilities, intrusion detection and response, and other services desired for ensuring the integrity of data and strategic IT assets.
>
> **Strategy 2** – The state must develop adequate disaster recovery and business continuity provisions for its strategic computing and telecommunications assets and mission-critical systems, with current and tested policies, procedures, and off-site backup facilities. Applications using distributed (non-mainframe) computing hardware/software and locally based telecommunications equipment must receive particular attention, as they are not adequately covered under current practices and capabilities.

Fifth Initiative – Find adequate, consistent, and reliable funding sources for IT investments and operations and the management of these.

Description

IT investments are necessary for enabling changes in the state's strategic goals and direction and program offerings and operations. These changes are required for the state to maintain relevance, sustain the trust and esteem of its citizens, and grow in its ability to serve its constituents. The continuous evolution of government services is driven by legal mandates; governmental initiatives; dramatic changes in the economic environment; and increasing demands of the public for additional services, greater convenience in dealing with government, and a better quality of life.

The understanding of and appreciation for the direct links among agency missions and strategies, program goals and objectives, and the management of IT investments and operations are absolutely essential prerequisites for

establishing a robust and effective IT investment management program. These relations are symbiotic. Agencies and programs cannot improve services, add new ones, or become more efficient or effective without an enabling and supporting IT infrastructure. Likewise, IT investments can only deliver value or benefits through the achievement of improvements in the processes, results, and outcomes of agency strategies and program operations.

The four types of IT investments typically found in state government are highlighted below:

- Implementations or renewals of common, shared technical infrastructure - statewide investments to support multiple applications for all agencies. By themselves, these investments may not necessarily offer economic value or citizen service benefits; however, they allow agency or business/program IT investments to do so in the most cost-effective, timely, and reliable manner.

- Implementations of new applications - agency or business/program opportunities to reduce expenses (increase productivity), offer new or improved services, and/or satisfy political mandates.

- Agency continuation funding for routine maintenance of applications or hardware/software replacement – ongoing funding for maintaining "as is" operations.

- Technology assessments - testing of opportunities for using new or emerging technologies to provide value or usefulness to the state.

By practicing astute capital planning and sound investment management, investments in technology can continue to support more informed management decisions; streamline, transform, and significantly improve government operations (i.e., increase the efficiency and effectiveness of processes and procedures); elevate the performance of programs; and enhance the delivery of goods and services to the public. The intent is to accomplish major objectives for managing IT as a statewide utility, which are:

- Identify and select high-value technology investments (including statewide common, shared infrastructure) that contribute to tangible, observable improvements in government performance and public good will.

- Implement these investments in the most cost-effective manner, within reasonable time frames, and with successful outcomes by employing a risk-based and performance-driven management perspective.

- Operate and maintain statewide common, shared infrastructure and mission-critical hardware/software assets in an economical, reliable, and secure manner, so they perform satisfactorily and are recoverable from human-made or natural disasters.

- Review statewide common, shared infrastructure and mission-critical hardware/software assets periodically to evaluate their cost-effectiveness and risk-acceptability and determine optimal times for enhancements and retirement or replacement.

Unfortunately, in the public and private sectors, the types and timing of funding for IT investments and operations often are incongruent with the management of these investments. The unique features of IT investments, create this situation, and these are highlighted as follows:

- IT investments can be capital intensive, highly leveraged, and labor consuming - statewide applications implementation projects may cost millions of dollars, and ongoing support costs (including labor) can be substantial over the life of the investment. Equally important, IT investments typically involve large fixed costs; therefore, in order to take advantage of economies of scale, the number of users and/or volumes of transactions must be as high as possible to minimize unit costs.

- While one-time purchase and implementation costs may be considerable, ongoing operating and maintenance expenses are also significant – A lifetime funding stream is required to obtain the maximum benefits from these investments.

- Even though these investments may not physically wear out, their lifetimes are uncertain – Premature obsolescence may originate from many sources, including changes in technology, transformations in business or program requirements, or removal of vendor support for hardware/software underpinnings. An emerging issue is the retirement of support personnel, without adequate preparation for continuity of knowledge and succession planning. The state should consider removing barriers to the use of retirees to assist in software remediation.

- Economics of many investments are enhanced through reliable and continuous funding streams – Leases and seat management contracts may be more economical over the long term; however, these options cannot be considered without some degree of assuredness for ongoing funding.

- Many of these investments require consistent replacement cycles for maintaining their usefulness and providing maximum benefits – Vendors are constantly offering new editions of software and model of hardware. While these offer advantages, older versions often must be upgraded to be compatible with the newer ones; thereby, creating additional cost pressures. Also, new hardware/software requires training for users and support staff, which adds to the purchase price for the total cost of ownership.

Current state funding models are not responsive to the realities of IT investments and operations for the following reasons:

- Agencies have been given money to start new projects, but subsequent operating and support expenses are not funded. Therefore, they must ask for expansion budget funds to cover ongoing expenses.

- Funding for IT investments only by agency or program often leads to inefficiencies in spending and loss of synergies by not being able to combine fiscal resources from multiple sources to obtain the greatest benefits for multiple participants (and the state as a whole).

- Limitations in transferring funds between ongoing operations and new efforts hamper the ability of agencies to keep their portfolios current.

- There are no provisions for reinvesting operational savings or program productivities accrued from IT investments.

An additional and related consideration is the present practices for the review of statewide IT costs may offer opportunities for improvement. The Office of State Controller publishes a comprehensive report of IT expenditures, but it does not receive significant attention. Because of deficiencies in the state's core business management systems (including human resources), personnel costs in the report are not comprehensive.

Equally important, there is no complete process for IT expenditure review, including pre-expenditure approval, concurrent expenditure examination, and post expenditure evaluation. As a result, agencies may spend money on bad systems because they don't have funds for replacing them. Also, duplications of IT investments, inefficient IT operations, and incomplete use of common technical services and shared technical infrastructures are at risk for not being identified. Without adequate review of expenditure information, there is no true responsibility and accountability for the statewide management of IT investments throughout their lifecycles.

Implementation Strategies

Implementation strategies for addressing funding challenges are listed below.

> **Strategy 1** – Develop provisions for enterprise infrastructure funding that provides common technical services and shared technical infrastructure including security services and disaster recovery/business continuity for all agencies and all programs.
>
> **Strategy 2** – Develop provisions for ongoing funding for operating and maintaining (or replacing/updating) mission-critical systems and applications, especially those at-risk due to obsolescence or lack of technical support.
>
> **Strategy 3** – Develop procedures (including the involvement of the State CIO, State Budget Officer, and State Controller) for reviewing funding requests (regardless of source) and examining ongoing funding certifications and expenses from the statewide perspective to eliminate duplication of investments, minimize statewide IT operating expenses, and ensure adequate infrastructure is available for and used by all agencies.

Sixth Initiative – Recruit and retain a proficient and appropriately staffed IT workforce.

Description

The lack of adequate personnel resources is a continuing and growing problem, and it is beginning to place applications and operations at risk. Some agencies are having difficulty transitioning from their legacy-oriented and mainframe-based technical infrastructure to today's distributed-asset and Internet/network-intensive technologies. The current state budget crisis is exacerbating the problem, with the elimination of key positions and the

reduction in funds for training. This challenge is compounded by the fact that many agency technical workers are reaching retirement age; therefore, succession planning and knowledge continuity for legacy applications are becoming increasingly important issues.

Employee morale has been adversely impacted by the cost cutting results of the state's perilous fiscal status. Workloads are increasing, the purchase of supporting tools and updated technologies have been postponed, and employee wealth has diminished by delayed salary increases and reduced health benefits.

While some agencies have been able to use outsourcing contracts for personnel services to address these situations, others have not possessed the financial wherewithal to exercise this option. Moreover, this approach is not cost-effective in all situations, and it ignores the longer-term problem of appropriate statewide IT personnel resource management.

State government is becoming more complex and agencies and programs are increasingly more interconnected. To be successful and productive, IT employees must continually adapt to changing technologies, new governmental initiatives, more demanding expectations for higher levels of program operations and successful outcomes, and mounting economic pressures and additional budget constraints. Static IT jobs no longer exist, and continually evolving roles and responsibilities have become the norm. Technical skills are not enough to cope with this ever-changing environment. Additional skills and abilities in the areas of collaborative work, interpersonal relations, and continuous learning are required for IT personnel to be active contributors in state government today.

Recent studies and experiences in the public sector and private industry point out that flexibility in the administration of personnel policies can assist in the ability of organizations to recruit, retain, and manage human capital. Areas where flexibilities have proven to be effective include hiring processes, acquiring and retaining temporary employees, recruitment and retention incentives, career development initiatives, performance management, compensation schemes, alternative work schedules, workplace realignment and job restructuring, position reclassification, and incentive awards and recognition.

An additional consideration for strategic workforce management is today's IT workforce is more than state employees. It includes contractors, consultants, citizen customers, business partners, and suppliers. All of these must be considered as part of the state's human capital and leveraged to create cost-effective and high-performance IT teams and organizations.

Implementation Strategies

The world of technology is one of unremitting change and incessant challenges. The state must establish what competencies and skills the IT workforce will need to meet future challenges, and it must develop the hiring practices and training and education opportunities to obtain, retain, and maintain these capabilities. The strategies below will assist the state to ensure it has sufficient numbers of IT personnel in place with the right skills, tools, and incentives to accomplish agency missions and program goals and objectives.

Strategy 1 – Research, develop, and fund programs for attracting and retaining qualified IT professionals, including competitive payment for required skills and abilities.

Strategy 2 – Ensure that agency technical staff and support personnel receive sufficient training to maintain agency IT assets and applications and acquire the knowledge and interpersonal skills necessary to adapt quickly to new technologies and the changing workplace environment.

Appendix – Agency Technology Plan for Information technology Services

States are recognizing the need to apply advanced information technology (IT) to improve government operations, offer more secure and responsive services to constituents, and further the democratic process. Over the years, North Carolina has made steady advances in building the governance structure, the technical infrastructure, and the enterprise approach to enable the cost-effective investment and efficient operation of technology necessary for the electronic delivery of services.

Recently, this progress has been slowed due to the confluence of a depressed and changing economy and the onslaught of expensive natural disasters, which have lead to a prolonged and severe budget crisis. With continued strong leadership, ongoing commitment of funding bodies, success in obtaining new and innovative sources of funds, and the proper allocation and application of fiscal and personnel resources, forward movement can be maintained, hopefully with increased momentum and greater steadfastness of purpose.

ITS has a central and pivotal role in the management of IT in state government. As a receipt supported entity providing computing, telecommunications and other technology related services to its state agency and local government customers, ITS must operate in a manner similar to a commercial organization in the private sector. As such, it must serve a useful purpose by meeting the needs of its clients with the levels of service desired by them at prices they can afford to pay. As a going concern without state appropriations, it must employ a viable business model, based on break-even pricing of services offered.

A new approach is required to address today's economic environment, business challenges, and technical possibilities. ITS must step forward with major initiatives and key supporting projects in order to:

- Support the business activities and program operations of the agencies.
- Enable more informed management decisions by state executives.
- Streamline, transform, and increase the efficiency and effectiveness of government processes and procedures.

- Elevate the performance of programs, with better outcomes and more desired results.

- Enhance the delivery of goods and services to the public.

Accordingly, eight major challenges have been identified that must be addressed in the near future. These originated from work with the clients, including the review of agency expansion budget requests, examination of agency IT plans, research of materials from leading IT advisory service organizations and current literature, and direct discussion and input from the ITS management team. They are in concert with the initiatives of the companion document, the Governor's and the IRMC's Statewide Strategies and Initiatives for the 2003-2005 Biennium.

While many of these challenges are continuation of past efforts, several are new or emerging issues that must be addressed soon in a thorough but prudent manner. This includes the transformation of the internal ITS culture to one that is more customer-centered, action-driven, project-oriented, and performance-measured. All eight are important, and the numbering is for organization only – it does not indicate rank, priority or sequence.

1. **Strengthen security approaches and capabilities** – The security of assets, confidentiality of data, and privacy of individuals are becoming more important in the management and operation of IT. ITS must build upon past advances to recognize more clearly the urgency for accelerated action, quicken the pace of progress in the state's security program, and shift its focus from planning to implementation.

2. **Expand disaster recovery and business continuity capabilities** – Natural and person-made disasters and accidents are not strangers to this state; therefore, ITS must enlarge present disaster recovery capabilities and services for mainframe-based applications to include distributed applications and associated assets, such as servers, desktops and communications equipment.

3. **Improve customer relations** – To remain in business, ITS must solve the technology problems and challenges of its customers; therefore, it must become more aware of the value of its customer-base to the organization and appreciate better its mission of helping its customers employ technology efficiently and effectively for meeting political initiatives, governmental mandates, and citizen expectations.

4. **Promote operational excellence and enhance service delivery** – In order to remain viable and prosper in the new technical world of integrated computing networks, ITS must change dramatically the ways it supports internal computing and telecommunications operations and the manner it delivers other services to its clients. It must do this by becoming more customer-aware, business-oriented, and disciplined-managed and by employing new forms of leadership, culture, processes, tools, and technical skills.

5. **Enhance statewide technical infrastructure services** – Organizations in both public and private sectors have show that the use of shared technical infrastructures and common technical services reduces costs, enhances service levels, and improves productivity and utilization of hardware/software and personnel resources. ITS must build upon its past statewide infrastructure implementations for e-government to meet emerging agency needs for security and the delivery of enhanced electronic services to the public.

6. **Expand support for statewide IT architecture and project management services** – Technical architectures and project management capabilities are critical success factors for the management, implementation and operation of IT investments. Therefore, ITS must move forward purposefully and quickly with its efforts to refresh and enhance the statewide technical architecture, improve project certification and management practices, and offer greater assistance to the agencies in implementing technical standards and approaches and acquiring project management skills.

7. **Improve administrative and support services** – Financial, personnel, and purchasing services are the essential underpinnings of the ITS organization; therefore, focused and high-priority projects and efforts must be performed expeditiously and successfully to improve the rate setting process, replace the outdated service billing application, manage succession and enhance employee morale and training, and add value to internal and statewide purchasing.

8. **Develop a comprehensive statewide outsourcing strategy by expanding lessons learned from past successful efforts** - Outsourcing is becoming a more popular mechanism for government at all levels to satisfy service delivery requirements in situations of constrained budgets; scarce, expensive, or hard-to-obtain personnel or technical resources; and/or time-sensitive implementations. Selective outsourcing of commodity-like services has proven to be a viable approach in situations where there are competing suppliers, known

specifications and requirements, and lack of satisfactory in-house capabilities; however, a comprehensive sourcing strategy, vendor contracting skills, and supplier management expertise are absolute prerequisites for success. ITS must be prepared to use the most cost-effective ways for employing IT to enable the delivery of public services, including the experiences of its many years of successful outsourcing engagements in telecommunications and other areas.